

DOR
8.370

Dorn Schuffman, Department Director

CHAPTER Regulatory Compliance	SUBCHAPTER HIPAA Regulation	EFFECTIVE DATE 10-15-2004	NUMBER OF PAGES 3	PAGE NUMBER 1 of 3
SUBJECT Security Maintenance		AUTHORITY 630.050	History: See below	
PERSON RESPONSIBLE Director of Information Systems			SUNSET DATE 7-1-2008	

Purpose: The Missouri Department of Mental Health is committed to maintaining formal practices to monitor the receipt and removal of hardware and electronic media that may contain electronic protected health information into and out of its facilities. The Department of Mental Health shall continue to develop, implement and maintain appropriate administrative, physical and technical security measures in accordance with 45 CFR 164.310(d).

Application: Applies to the Department of Mental Health, its' facilities and its' workforce.

(1) Contents

- (A) Definitions
- (B) General
- (C) Procedures
- (D) Derivative Documents
- (E) DOR Control
- (F) Sanctions
- (G) Review Process

(2) Definitions

(A) DMH Workforce – Includes employees, volunteers, contract workers, interns, trainees and other persons who are in a DMH facility or Central Office on a regular course of business. This shall include client workers employed by the DMH or any of its facilities.

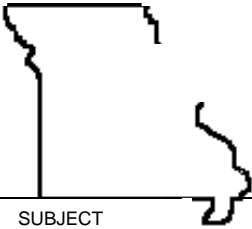
(B) Local Security Officer (LSO) – Individual designated by a facility CEO to oversee facility information and physical security practice and policy compliance and to coordinate those activities with the Chief Security Officer

(C) Chief Security Officer (CSO) – Individual designated by the DMH to oversee all activities related to the development, implementation, maintenance of, and adherence to department and facility policies and procedures covering the electronic and physical security of, and access to, protected health information and other DMH data in compliance with federal and state laws and regulations

(D) Electronic Protected Health Information (E-PHI) — individually identifiable health information that is transmitted or maintained in electronic media; or transmitted or maintained in any other form or medium.

(E) Sensitive Items – Hardware items under \$1000.00, but are considered potentially high theft items.

(F) Master Inventory List – DMH Information Technology Hardware and Software Database.



DORN SCHUFFMAN, DEPARTMENT DIRECTOR



DOR
8.370

SUBJECT Security Maintenance	EFFECTIVE DATE October 15, 2004	NUMBER OF PAGES 3	2 of 3
---------------------------------	------------------------------------	----------------------	--------

(3) General

(A) The policies and procedures stated herein apply to all electronic protected health information maintained or transmitted by the Department of Mental Health.

(B) Receipt, removal, back-up, storage, re-use and disposal of electronic protected health information into or out of a facility, as well as throughout the facilities operated by the Department of Mental Health shall be governed by the policies and procedures herein.

(C) The policies and procedures herein also apply to the hardware on which data is stored.

(4) Procedures

(A) Procedures for receiving hardware into a facility:

1. A record shall be maintained by receiving personnel documenting all hardware received into the facility using form Receiving Report of Nonexpendable Property MO 650-0184N. Receiving personnel shall provide a receipt and/or signature to the deliverer to document obtaining such components in acceptable condition.

2. Receiving personnel shall property tag all hardware items with a value exceeding \$1000.00 or sensitive items with a unique property number identifier per facility.

3. Receiving personnel shall deliver any hardware to the Information Technology section for installation.

4. The LSO or designee shall use automation to install standard software to include virus protection on all hardware to be used by Department of Mental Health workforce. This does not preclude using non-automation for non-standard software or individual use packages.

5. The LSO or designee shall ensure the master inventory list is updated and fixed asset personnel are notified.

(B) Procedures for transferring hardware from a facility:

1. Written approval must first be obtained by completing form Authorization for Property Release MO 650-7876 or Property Possession Form MO 650-2794.

2. The LSO or designee shall ensure the master inventory list is updated with off-site information.

(C) Procedures for backing up and storing hardware and/or software containing protected health information:

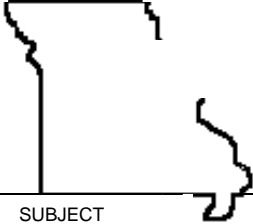

1. Determine when backups are needed prior to movement of equipment.
2. Make an exact, retrievable copy of the data on a network server and restrict access.

3. Test the copy to ensure the copy is exact and retrievable.

4. Make sure these files are included on the nightly server backup.

5. Ensure backups are stored in a secure location and are also kept off-site in accordance with DMH backup procedures.

(D) Procedures for disposing of electronic data, including hardware and/or software on which data is stored:

	DORN SCHUFFMAN, DEPARTMENT DIRECTOR		DOR 8.370
SUBJECT Security Maintenance	EFFECTIVE DATE October 15, 2004	NUMBER OF PAGES 3	3 of 3

1. The LSO or designee shall ensure protected health information has been destroyed. For procedures for the destruction of computer disk, laser disks, back-up tapes, etc., refer to the destruction requirements as set forth in DOR 8.330.

2. The disposal of hardware shall require a completed Property Movement/Disposition form MO 650-0051.

3. The master inventory list shall be updated and the appointed Receiving Fixed Asset Contact shall sign for accuracy.

(E) Procedures for the re-use of media and devices that contain electronic protected health information, including hardware and/or software on which such data is stored:

1. The LSO or designee shall use Symantec Ghost imaging software to install a Ghost image to overwrite any data to include personal health information. This shall ensure no data can be retrieved by using this method.

2. The LSO or designee shall use the Disk Wipe procedures outlined in the OIS Standards List for servers that may include protected health information.

3. The LSO or designee shall complete a Property Movement/Disposition form MO 650-0051.

4. The master Inventory list shall be updated and the appointed Receiving Fixed Asset Contact shall sign for accuracy.

(F) Accountability Procedures:

1. Having identified the applicable components, and in accordance with the above procedures, maintain a record of the movements of hardware, electronic media and devices and the associated responsible persons (the LSO or designee, receiving personnel and receiving fixed asset personnel).

2. Ensure the records are kept up-to-date and secured.

(5) Derivative Documents - The policies and procedures established herein, including all derivative documents regarding receipt, removal, storage and/or disposal of electronic data, hardware, and/or software into or out of a facility operated by the Department of Mental Health shall be documented and maintained in a current manner.

(6) DOR Control - There shall be no facility policies pertaining to this topic. The Department Operating Regulations shall control.

(7) Sanctions. Failure of workforce members to comply or ensure compliance with the DOR may result in disciplinary action, up to and including dismissal.

(8) Review Process. The Chief Security Officer shall assign regular checks to see that all hardware and software receipt is done in accordance with these policies and procedures, and take corrective action as necessary.

History: Original rule effective October 15, 2004.